MULTIMEDIA UNIVERSITY®

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2019/2020

ECE3256 CYBERSECURITY

(All Sections / Groups)

28 FEBRUARY 2020
9:00 A.M – 11:00 A.M.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 7 printed pages including the cover page with 4 questions only.

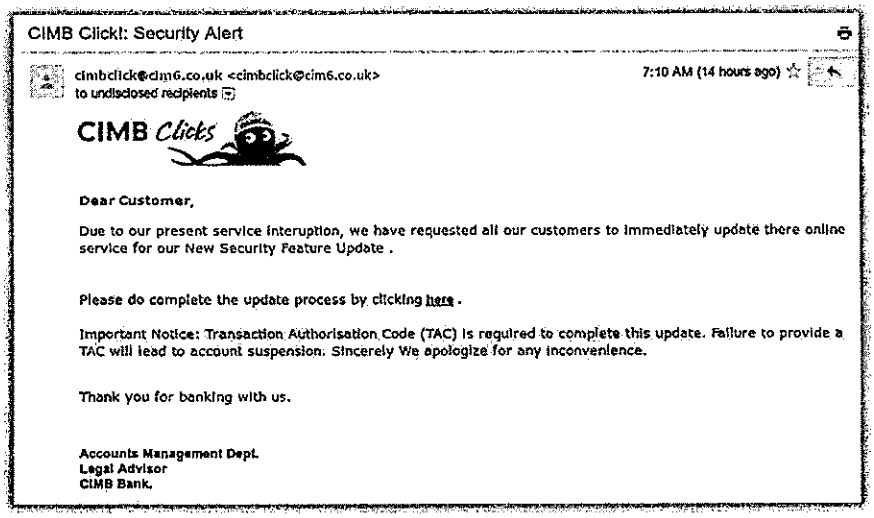
2. Attempt all FOUR (4) questions. All questions carry equal marks and the distribution of marks is given in the questions.

3. Please print all your answers in the answer booklet provided.

4. State all assumptions clearly.

Question 1

(a) You received an urgent email out of the blue from a bank as shown in Figure Q1(a).


CIMB Click!: Security Alert

cimbclick@cim6.co.uk <cimbclick@cim6.co.uk> 7:10 AM (14 hours ago)
to undisclosed recipients

CIMB Clicks

Dear Customer,

Due to our present service interuption, we have requested all our customers to immediately update there online service for our New Security Feature Update .

Please do complete the update process by clicking here .

Important Notice: Transaction Authorisation Code (TAC) is required to complete this update. Failure to provide a TAC will lead to account suspension. Sincerely We apologize for any inconvenience.

Thank you for banking with us.

Accounts Management Dept.
Legal Advisor
CIMB Bank.

Figure Q1(a)

(i) Is the email legitimate or otherwise?

[1 mark]

(ii) Justify your answer in Part (i) by describing at least **THREE (3)** signs or indicators that may indicate whether the email is legitimate or otherwise.

[6 marks]

(b) List and briefly explain the **THREE (3)** goals of Cybersecurity.

[6 marks]

(c) Social Engineering is a type of cybersecurity attack.

- Describe this type of attack.

[2 marks]

- What are the **FOUR (4)** psychological traits that attackers exploit to launch this attack?

[4 marks]

- Briefly describe an example or scenario where this attack is used.

[3 marks]

(d) Describe the concept of Defense-in-Depth and provide examples of how each "depth" can be achieved.

[3 marks]

Continued...

Question 2

(a) Why is it a best practice to transmit the hash of a password instead of the password itself? How does *Kerckhoff's Principle* relate to this practice?

[2 marks]

(b) The Multiplicative Cipher is a type of monoalphabetic cipher.

(i) Write the corresponding decryption formula if the encryption formula is written as:

$$C = E(P) = (11 \cdot P) \bmod 26$$

[Note: You do not need to calculate the multiplicative inverse yet.]

[1 mark]

(ii) Explain why $k = 11$ is a suitable key for the multiplicative cipher in Part (i).

[2 marks]

(iii) Calculate the multiplicative inverse of 11 mod 26 using the trial and error method. Show all your steps, including the calculations to obtain the answer.

[3 marks]

(iv) Decrypt the following word using the $k = 11$. Show your steps to decrypt the word.

JSANMB

[3 marks]

(c) Using AES, perform the following operations.

(i) Express the following plaintext and secret key as an AES state.

Plaintext: {6B C1 BE E2 2E 40 9F 96 E9 3D 7E 11 73 93 17 2A}

[1 mark]

(ii) Assume that the plaintext state in Part (i) is the input into AES' SubBytes function. Show the new state after **SubBytes** using the S-Box in Figure Q2(c).

[3 marks]

(iii) Subsequently, show the output state after the **ShiftRows** function is applied on the results of Part (ii).

[3 marks]

Continued...

hex	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

x

The Substitution Table – Sbox[xy] (in hexadecimal)

Figure Q2(c)

(d) Consider the RSA cryptosystem with $p = 5$, $q = 11$ and $e = 7$.

(i) Find the corresponding decryption key, d using the given parameters.

[3 marks]

(ii) Write down the formulas for encryption and decryption

[2 marks]

(iii) Subsequently, encrypt the message, $m = 4$ using the appropriate formula from Part (ii)

[2 marks]

Continued...

Question 3

(a) After studying the logs of the company's computers (servers and workstations), you noticed that computers are systematically **scanned** for opened ports. Other than that, everything else is normal and there had not been any cybersecurity incidences.

(i) What is the name of this activity?

[1 mark]

(ii) What are the goals or objectives of this activity?

[2 marks]

(iii) Is this a type of active or passive attack? Justify your answer.

[2 marks]

(iv) How can you mitigate this type of activity?

[2 marks]

(b) Describe the following types of active network attacks and **ONE (1)** of their corresponding mitigation methods

(i) Denial-of-Service (DDoS)

[3 marks]

(ii) Evil Twin Access Point

[3 marks]

(c) As the new Security Officer in your organisation, you have to explain to Management why an IDS is needed to protect the organisation's network.

(i) In the context of network security, what does IDS stand for?

[1 mark]

(ii) Briefly describe the general purpose of an IDS.

[3 marks]

(iii) Name and explain the **TWO (2)** categories of IDS based on **what they monitor.**

[4 marks]

(iv) Name and explain the **TWO (2)** categories of IDS based on **how they function.**

[4 marks]

Continued...

Question 4

(a) Briefly explain the following types of malware.

(i) Virus

[2 marks]

(ii) Trojan Horse

[2 marks]

(iii) Backdoor

[2 marks]

(iv) Worm

[2 marks]

(v) Ransomware

[2 marks]

(b) KK Grocery is a small business with a webserver that hosts a basic website. The website displays products and their corresponding quantity and prices but does not carry out any e-commerce transactions. The webpage is updated daily at the end of business hours to reflect the latest inventory.

Describe a backup strategy that includes the type of backup, frequency of backups, and your justifications.

[3 marks]

(c) Design a layered security strategy to protect the company's computing infrastructure shown in Figure Q4(c). To do this, explain at least **FOUR (4)** tools (e.g. software, devices, policies) that could be used. Your explanation for each of the tool should contain:

(i) A brief description of each tool

[4×1 marks]

(ii) How it protects the computing infrastructure

[4×1 marks]

(iii) Where the tool should be placed in the network. Redraw Figure Q4(c) in your answer booklet after the security tool has been properly added.

[4×1 marks]

Continued...

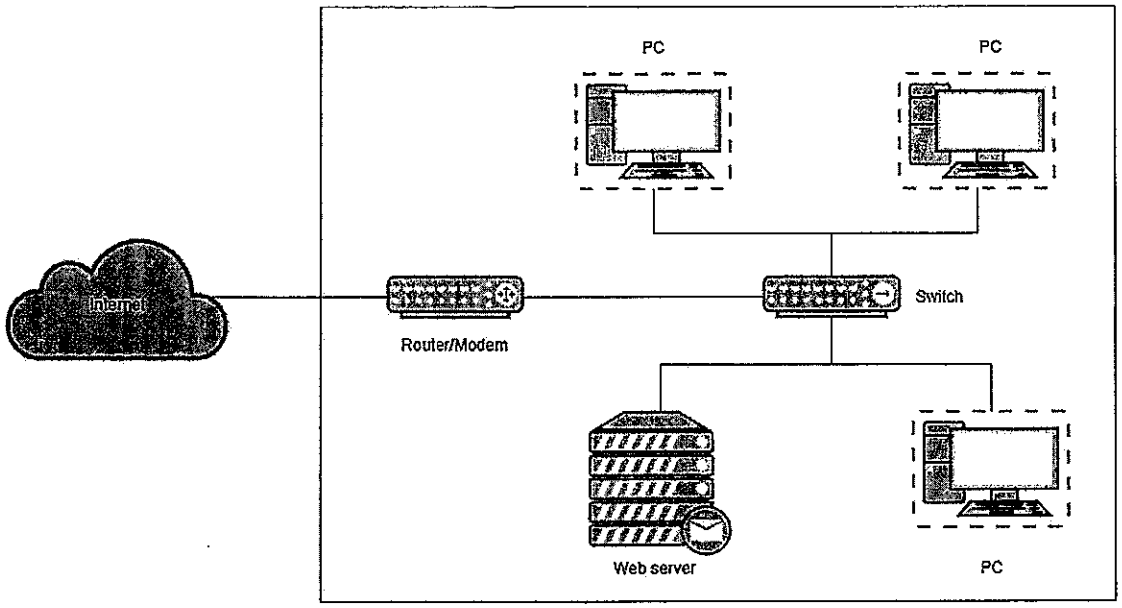


Figure Q4(c)

End